IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IPA TECHNOLOGIES, INC., Plaintiff, v. AMAZON.COM, INC., and AMAZON DIGITAL SERVICES, LLC, Defendants.	C.A. No. 16-1266-RGA
IPA TECHNOLOGIES, INC., Plaintiff, v. MICROSOFT CORPORATION, Defendant.	C.A. No. 18-01-RGA
IPA TECHNOLOGIES, INC., Plaintiff, v. GOOGLE LLC, Defendant.	C.A. No. 18-318-RGA

[STIPULATED] ORDER RE: DEFAULT STANDARD FOR DISCOVERY, INCLUDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION ("ESI")

1. Purpose. This Order will govern discovery of electronically stored information ("ESI") in this case as a supplement to the Federal Rules of Civil Procedure and any other applicable orders and rules.

2. General Provisions.

a. **Cooperation.** Parties are expected to reach agreements cooperatively on how to conduct discovery under Fed. R. Civ. P. 26-36. In the event that the parties are unable to agree on the parameters and/or timing of discovery, the following default standards shall apply until further order of the Court or the parties reach agreement.

b. **Proportionality.** Parties are expected to use reasonable, good faith and proportional efforts to preserve, identify and produce relevant and reasonably accessible information.[1] This includes identifying appropriate limits to discovery, including limits on custodians, identification of relevant subject matter, time periods for discovery and other parameters to limit and guide preservation and discovery issues; provided, however, that if a party desires discovery from sources outside the United States, the parties shall meet and confer on the necessity of such discovery and any limits or protections needed due to privacy and other laws.

c. **Preservation of Discoverable Information.** A party has a common law obligation to take reasonable and proportional steps to preserve discoverable information in the party's possession, custody or control.

(i) Absent a showing of good cause by the requesting party, the parties shall not be required to modify, on a going-forward basis, the procedures used by them in the ordinary course of business to back up and archive data; provided, however, that the parties shall take reasonable steps to preserve the non-duplicative discoverable information currently in their possession, custody or control.

[1] Information can originate in any form, including ESI and paper, and is not limited to information created or stored electronically.

(ii) The producing party is not required to preserve or search email and file servers temporarily replicated for disaster recovery, backup, or business continuity purposes, obsolete media, legacy systems, and sources requiring computer forensic analysis.

(iii) Absent a showing of good cause by the requesting party, the categories of ESI identified in Schedule A attached hereto need not be preserved.

d. **Privilege.**

(i) The parties are to confer on the nature and scope of privilege logs for the case, including whether categories of information may be excluded from any logging requirements and whether alternatives to document-by-document logs can be exchanged.

(ii) With respect to information generated after the filing of the complaint, parties are not required to include any such information in privilege logs.

(iii) Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Fed. R. Civ. P. 26(b)(3)(A) and (B).

(iv) Pursuant to Fed. R. Evid. 502(d), the production of a privileged or work-product-protected document is not a waiver of privilege or protection from discovery in this case or in any other federal or state proceeding. For example, the mere production of privilege or work-product-protected documents in this case as part of a mass production is not itself a waiver in this case or any other federal or state proceeding. Information that contains privileged matter or attorney work product shall be immediately returned if such information appears on its face to have been inadvertently produced or if notice is provided of inadvertent production.

3. Initial Discovery Conference.

a. **Timing.** Consistent with the guidelines that follow, the parties shall discuss the parameters of their anticipated discovery at the initial discovery conference (the "Initial

Discovery Conference") pursuant to Fed. R. Civ. P. 26(f), which shall take place before the Fed. R. Civ. P. 16 scheduling conference ("Rule 16 Conference") or at the time specified in the Pretrial Scheduling Order to be entered by the Court.

b. **Content.** The parties shall discuss the following:

(i) The issues, claims and defenses asserted in the case that define the scope of discovery.

(ii) The likely sources of potentially relevant information (i.e., the "discoverable information"), including witnesses, custodians and other data sources (e.g., paper files, email, databases, servers, etc.).

(iii) Technical information, including the exchange of production formats.

(iii) The existence and handling of privileged information.

(iv) The categories of ESI that should be preserved.

4. Initial Disclosures. Within 30 days after the Rule 16 Conference or within a timeframe to be established, each party shall disclose:

a. **Custodians.** The 10 custodians most likely to have discoverable information in their possession, custody or control, from the most likely to the least likely. If, after a reasonable search, a party does not have ten such custodians likely to have non-duplicative, discoverable information, then ten custodians do not have to be identified. The custodians shall be identified by name, title, role in the instant dispute, and the subject matter of the information.[2]

b. **Non-custodial data sources.**[3] A list of the non-custodial data sources that are most

[2] As these disclosures are "initial," each party shall be permitted to supplement.
[3] That is, a system or container that stores ESI, but over which an individual custodian does not organize, manage or maintain the ESI in the system or container (e.g., enterprise system or database).

likely to contain non-duplicative discoverable information for preservation and production consideration, from the most likely to the least likely.

c. **Notice.** The parties shall identify any issues relating to:

(i) Any additional sources of ESI not identified in this Order or Schedule A (by type, date, custodian, electronic system or other criteria) that a party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(C)(i).

(ii) Third-party discovery under Fed. R. Civ. P. 45 and otherwise, including the timing and sequencing of such discovery.

(iii) Production of information subject to privacy protections, including information that may need to be produced from outside of the United States and subject to foreign laws.

Lack of proper notice of such issues may result in a party losing the ability to pursue or to protect such information.

5. Initial Discovery in Patent Litigation.[4]

a. Within 30 days after the Rule 16 Conference or as otherwise agreed by the parties and for each defendant,[5] the plaintiff shall specifically identify the accused products[6] and the asserted patent(s) they allegedly infringe, and produce the file history for each asserted patent.

b. Within 30 days after receipt of the above or as otherwise agreed by the parties, each defendant shall produce to the plaintiff core technical documents related to the accused product(s), including but not limited to operation manuals, product literature, schematics, and/or

[4] As these disclosures are "initial," each party shall be permitted to supplement.
[5] For ease of reference, "defendant" is used to identify the alleged infringer and "plaintiff" to identify the patentee.
[6] For ease of reference, the word "product" encompasses accused methods and systems as well.

specifications.

c. Within 30 days after receipt of the above or as otherwise agreed by the parties, plaintiff shall produce to each defendant an initial claim chart relating each accused product to the asserted claims each product allegedly infringes.

d. Within 30 days after receipt of the above or as otherwise agreed by the parties, each defendant shall produce to the plaintiff its initial invalidity contentions for each asserted claim, as well as the related invalidating references (e.g., publications, manuals and patents).

e. Absent a showing of good cause, follow-up discovery shall be limited to a term of 6 years before the filing of the complaint, except that discovery related to asserted prior art or the conception and reduction to practice of the inventions claimed in any patent-in-suit shall not be so limited.

6. Specific E-Discovery Issues.

a. **On-site inspection of electronic media.** Such an inspection shall not be permitted absent a demonstration by the requesting party of specific need and good cause.

b. **Search methodology.**

(i) If the producing party elects to use search terms to locate potentially responsive ESI, it shall disclose the search terms to the requesting party. Absent a showing of good cause, a requesting party may request no more than 10 additional terms to be used in connection with the electronic search. Focused terms, rather than over-broad terms (e.g., product and company names), shall be employed. The parties shall meet and confer on any modifications to the proposed terms needed to improve their efficacy in locating discoverable information and in excluding information that is not discoverable under Fed. R. Civ. P. 26(b), including modifying terms where the burden or expense of the proposed terms outweighs the likely benefit.

The producing party shall search (i) the non-custodial data sources identified in accordance with paragraph 4(b); and (ii) emails and other ESI maintained by the custodians identified in accordance with paragraph 4(a).

(ii) Each party will use its best efforts to filter out common system files and application executable files by using a commercially reasonable hash identification process. Hash values that may be filtered out during this process are located in the National Software Reference Library ("NSRL") NIST hash set list. Additional culling of system file types based on file extension may include, but are not limited to: WINNT, LOGS, DRVS, Channel Definition Format (cdf), Creatures Object Sources (cos), Label Pro Data File (IPD), Office Data File (NICK), Office Profile Settings (ops), Outlook Rules Wizard File (rwz), Scrap Object, System File (dll), Temporary File (tmp), Windows Error Dump (dmp), Windows Media Player Skin Package (wmz), Windows NT/2000 Event View Log file (evt).

(iii) Each party may produce only a single copy of a responsive document and each party may de-duplicate responsive ESI (based on MD5 or SHA-1 hash values at the document level) across custodians; however, the identity of each custodian possessing the de-duplicated document must be identified in production .For emails with attachments, the hash value is generated based on the parent/child document grouping. A party may also de-duplicate "near-duplicate" email threads as follows: In an email thread, only the final-in-time document need be produced, assuming that all previous emails in the thread are contained within the final message. Where a prior email contains an attachment, that email and attachment shall not be removed as a "near-duplicate." To the extent that de-duplication through MD5 or SHA-1 hash values is not possible, the parties shall meet and confer to discuss any other proposed method of de-deduplication.

c. **Format.** ESI and non-ESI shall be produced to the requesting party as text searchable image files (e.g., PDF or TIFF). When a text-searchable image file is produced, the producing party must take reasonable steps to preserve the integrity of the underlying ESI, i.e., the original formatting , the metadata (as noted below) and, where applicable, the revision history. The parties shall produce their information in the following format: single page TIFF images and associated multi-page text files containing extracted text or OCR with Concordance and Opticon load files containing all requisite information including relevant metadata.

d. **Native Files**. The only files that should be produced in native format are files not easily converted to image format, such as Excel and Access files.

e. Metadata. The parties are only obligated to provide the following metadata for all ESI produced, to the extent such metadata exists and can be reasonably provided: Custodian, File Path, Email Subject, Conversation Index, From, To, CC, BCC, Date Sent, Time Sent, Date Received, Time Received, Filename, Author, Date Created, Date Modified, MD5 Hash, File Size, File Extension, Control Number Begin, Control Number End, Attachment Range, Attachment Begin, and Attachment End (or the equivalent thereof).

f. **Source Code.** No provision of this Order affects any inspection of source code that is responsive to a discovery request and will be made available consistent with the protective order governing this case.

7. Modification.

This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown. Any such modified Stipulated Order will be titled sequentially as follows, "First Modified Stipulated Order re: Discovery of Electronically Stored Information for

Standard Litigation," and each modified Stipulated Order will supersede the previous Stipulated Order.

BAYARD, P.A.

/s/ Stephen B. Brauerman
Stephen B. Brauerman (#4952)
Sara E. Bussiere (#5725)
600 North King Street, Suite 400
Wilmington, DE 19801
(302) 655-5000
sbrauerman@bayardlaw.com
sbussiere@bayardlaw.com

Attorneys for Plaintiff

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Rodger D. Smith
Jack B. Blumenfield (#1014)
Rodger D. Smith II (#3778)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
jblumenfeld@mnat.com
rsmith@mnat.com

Attorneys for Defendants Google, LLC and Microsoft Corp.

ASHBY & GEDDES

/s/ Andrew C. Mayo
Steven J. Balick (#2114)
Andrew C. Mayo (#5207)
500 Delaware Avenue, 8th Floor
P.O. Box 1150
Wilmington, DE 19899
(302) 654-1888
sbalick@ashby-geddes.com
amayo@ashby-geddes.com

Attorneys for Defendants Amazon.com, Inc. and Amazon Digital Services, LLC

IT IS SO ORDERED this 26 day of June, 2019.

Hon. Richard G. Andrews
United States District Judge

SCHEDULE A

1. Deleted, slack, fragmented, or other data only accessible by forensics.

2. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

3. On-line access data such as temporary internet files, history, cache, cookies, and the like.

4. Data in metadata fields that are frequently updated automatically, such as last- opened dates.

5. Automatically saved versions of documents and emails.

6. Back-up data that are substantially duplicative of data that are more accessible elsewhere or that is temporarily created for disaster recovery or business continuity purposes.

7. Voice messages.

8. Instant messages-that are not ordinarily printed or maintained in a server dedicated to instant messaging.

9. Electronic mail or pin-to-pin messages sent to or from mobile devices (e.g., iPhone and Blackberry devices).

10. Other electronic data stored on a mobile device.

11. Logs of calls made from mobile devices.

12. Server, system or network logs.

13. Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as part of a laboratory report.

14. Data remaining from systems no longer in use that is unintelligible on the systems in use.